Change Management Process Handbook

Document ID/CI Number: TBD
Version: 1.00
Issue Date: 01/26/2018

Revision History

Date	Version	Description	Author
09/06/2017	V0.1-0.3	- Initial Version - Base information from ChM Process Definition Document v1-2, July 2017 - Draft version .08	(b) (6)
11/02/2017	V0.4	Aligned with BPR Template	(b) (6)
11/23/2017	V0.5	Updated with feedback from Mark Breckenridge	(b) (6)
12 Dec 2017	V0.6	Updated with Feedback from Kris Hoffman	(b) (6)
7 Jan 2018	V0.7	Updated with additional feedback from Kris Hoffman to include expanding details on CAB and 2018 plan for formalizing the CAB as the official change authority/authorities.	(b) (6)
26 January 2018	V1.0	EGC Approved	(b) (6)

Review

Review Date	Reviewed By	Findings	Remarks/ Recommendations
23 Oct 2017	PM BPR Team	Grammar check and suggestions for reducing unneeded sections of the handbook.	Accepted the suggestions and made corrections
09 Nov 2017	(b) (6)	Grammar Check and Major Version Updates for EGC Approval	Updated for EGC Approval
21 Nov 2017	(b) (6)	Comments and edits	Align roles and integrate references in activities section
12 Dec 2017	(b) (6)	Comments and edits	Correct abbreviations, address role of CAB introduced, remove glossary.
4 Jan 2018	(b) (6)	Need for clarification of CAB Request to clarify instructions	Make clarifications and then move the document forward for

			review. Address CAB questions separately.

Approvals

The undersigned has/have reviewed this document and approve its contents.

Approver Name	Department/Role	Signature
(b) (6)	DMDC Technical Services Directorate Lead	(b) (6)
(b) (6) DMDC IT Operations Division Director	Division Director Change Management Process Owner	
(b) (6)	DMDC Deputy Director/ DMDC Director	

Contents

1. Introduction

Process Description

The Change Management (ChM) process is a *control* process. It acts to ensure the enforcement, control, coordination, management and governance of the service lifecycle. The Chm process works in close cooperation with Service Asset and Configuration Management (SACM) [another *control* process] and Release and Deployment Management.

2. Change Management Overview

2.1 Purpose

The purpose of the ChM process is to control the lifecycle of all changes that are in-scope for the process and to enable beneficial changes to be made with minimum disruption to DMDC services.

2.2 Goals

The ***goals*** of ChM process are to ensure that Information Technology (IT) implements all changes without any negative impact on customer service, which includes but are not limited to the following:

- Respond to the customer's changing business requirements while maximizing value and reducing incidents, disruption and re-work.
- Respond to the business and IT requests for change that will align the services with the business needs.
- Ensure that changes are recorded and evaluated, and that authorized changes are prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.
- Ensure that all changes to configuration items are recorded in the configuration management system (e.g., ITSM (IT Service Management) System)
- Facilitate change, while maintaining or improving system availability
- Determine whether the amount of lead time affects the success or failure of non-disruptive changes
- Reduce the number of changes requiring "back-out" due to inadequate preparation or defects
- Determine better methods for identifying and categorizing changes into levels of risk
- Display the number and types of changes planned in the short and long term
- Ensure that every change record has technical and management accountability to provide a compliance audit trail

- Establish a process to ensure that change requests are consistently reviewed for technical merit and business readiness, while allowing for flexibility based on business needs
- Avoid conflicts by holistically managing the scheduling of all changes

2.3 Accountability

The Change Management process was produced through a Business Process Review (BPR) led by the DMDC Technology Services Operations Director, Michele Bolinger, who served as Process Champion. Upon completion of the initial BPR, the Change Management process is to be transitioned to the Technical Services Operations.

2.4 Value to the DMDC Mission

Confidentiality, integrity, reliability and availability are essential for the success of DMDC, and service / infrastructure changes can have a negative impact on the DMDC business by disrupting services. The ChM process adds value to the business by:

- Protecting DMDC and DMDC services, while facilitating the efforts to make required changes
- Providing management for the implementation of configuration changes that meet the customers' agreed service requirements while optimizing costs
- Contributing to meet governance, legal, contractual and regulatory requirements by providing auditable evidence of change management activity.
- Reducing failed changes and therefore service disruption, defects and re-work
- Reducing the number of unauthorized changes, leading to reduced service disruption and reduced time to resolve change-related incidents
- Delivering change promptly to meet business timescales

2.5 Scope

By best practices, the scope of ChM is to cover changes to all established configuration items (CIs) across the enterprise, whether these CIs are physical assets such as servers or network devices, virtual assets such as virtual servers or virtual storage, or other types of assets such as software, applications, agreements or contracts.

2.5.1 In-Scope

This ChM process applies to the following DMDC systems and services, regardless of level or location:

- All DMDC services, systems, servers, networks, applications and software. This includes COTS (commercial off the shelf software) and GOTS (Government off the shelf software) as a part of service and applications' configurations.
- All facilities and environments managed by Technical Services Operations, to include data centers, network rooms, etc.

- Laptop/desktop operating system (OS) images and other operational level configuration items.

2.5.2 Not-In-Scope

The ChM process does not include the control for the following areas:

- Changes to other services, applications and/or systems not listed as being In-Scope for this process
- Changes with significantly wider impacts than service changes, e.g. departmental organization, policies and business operations
- Changes to desktops, laptops, printers or other components not directly related to service CIs.

3. Change Management High Level Process Activities

This section presents a high level overview of the Change Management process, using flow charts from Sparx Enterprise Architect, hereafter referred to as Sparx, to visually depict the activities, the order of those activities, and the roles responsible for conducting each activity. More detailed information about the specific activities associated with each step in the model is presented in the *Process Activity Description* section.

3.1. Process Inputs

- Policy and strategy for change and release
- Request for change
- Change proposal
- Plans – change, transition, release, test, evaluation and remediation
- Current change schedule and PSO
- Evaluation reports and interim evaluation reports
- Current assets or configuration items, e.g. baseline, service package, release package
- As-planned configuration baseline
- Test results, test report and evaluation report.
- Feedback from all other processes.

3.2. Process Outputs

- Disapproved and cancelled Change Requests (CRs)
- Authorized changes
- Change to the services, service or infrastructure resulting from authorized changes
- New, changed or disposed configuration items, e.g. baseline, service package, release package
- Revised change schedule
- Revised Projected Service Outages (PSO)

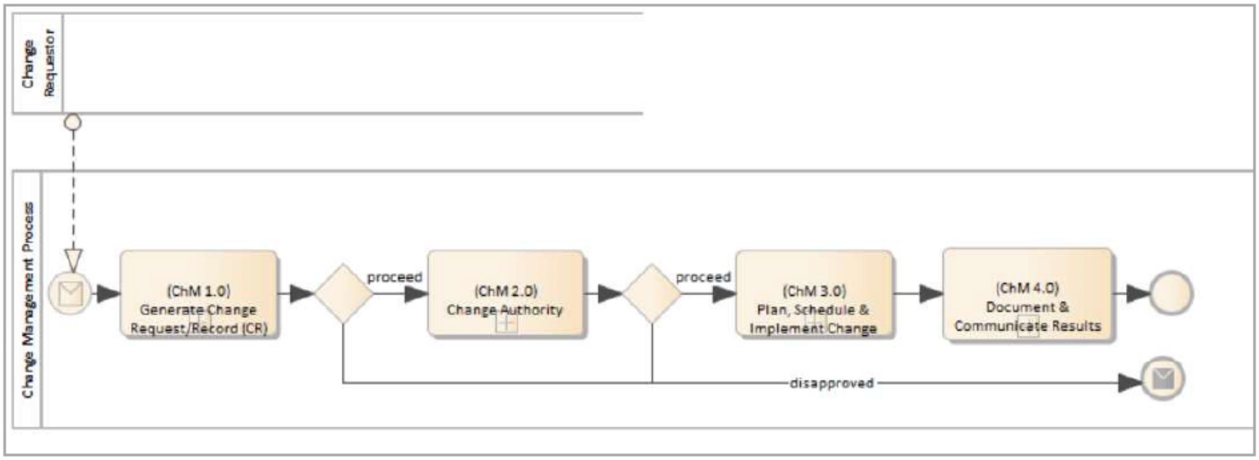
- Authorized change plans
- Updated disaster recovery plans
- Change decisions and actions
- Change documents and records
- Change management reports.

3.3. Process Activities

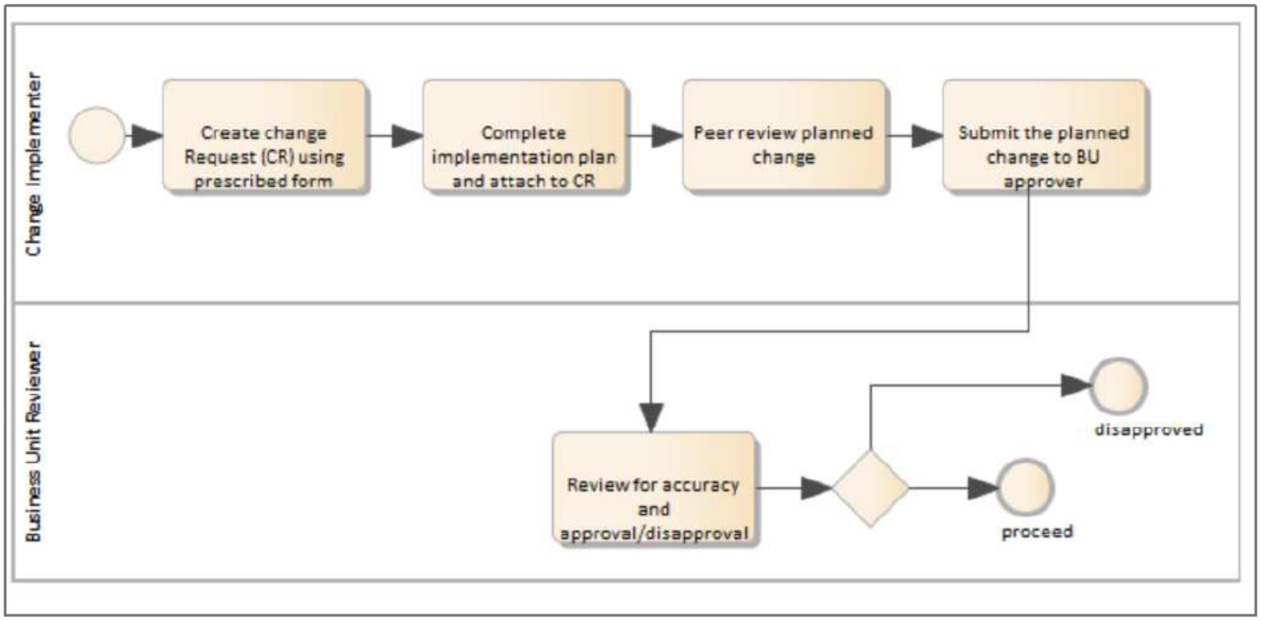
The following charts provide a high-level flow of the activities in the Change Management process and delineate activities that are owned by the various groups. These charts were generated from Sparx. The tables that follow each chart or charts provide a detailed description of each activity in the process to a level that is sufficient for personnel to accomplish the activities.

3.3.1. ChM Process Overview

The following figure represents the high-level end-to-end ChM process. In the sections that follow, each major step of the process is further decomposed and the high level activities described.


Change Requestor
Change Management Process
(ChM 1.0) Generate Change Request/Record (CR)
proceed
(ChM 2.0) Change Authority
proceed
(ChM 3.0) Plan, Schedule & Implement Change
(ChM 4.0) Document & Communicate Results
disapproved

3.3.2. Generate Change Request (ChM 1.0)

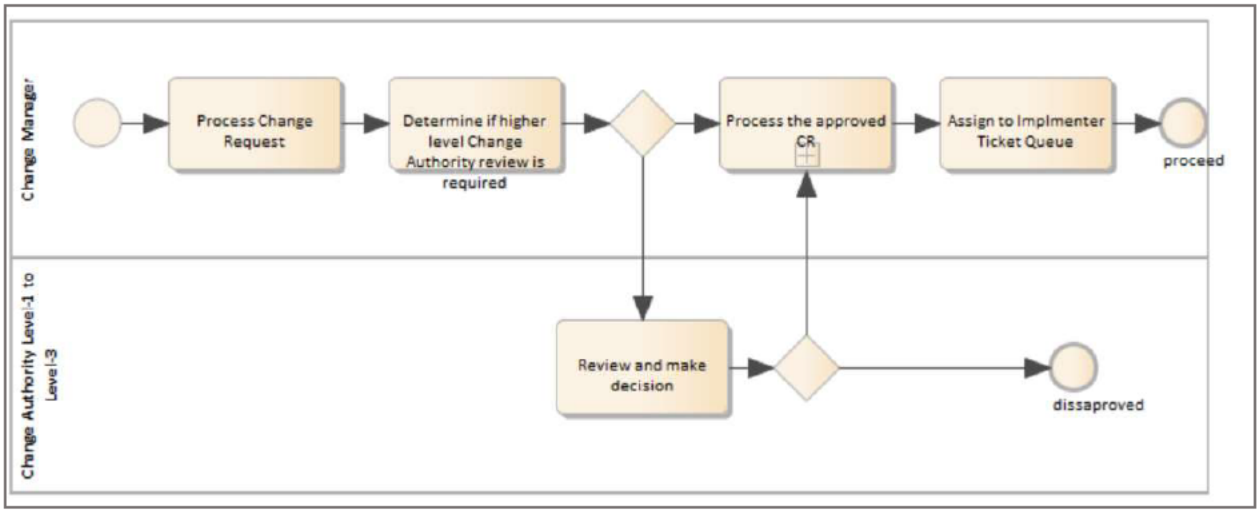

Change Implementer
Create change Request (CR) using prescribed form
Complete implementation plan and attach to CR
Peer review planned change
Submit the planned change to BU approver
Business Unit Reviewer
Review for accuracy and approval/disapproval
disapproved
proceed

	Activity	Description	Role
3.3.2.1	Create the Change Request (CR) (ChM 1.1)	Given requirement to make change to a configuration item (CI) or asset, the requester follows established instructions to create a change request (CR).	Change Requester
3.3.2.2	Create and complete implementation plan	If the Requester is not the Implementer, they will work with the Implementer to develop and complete the implementation plan, back-out plan, resource and communications plans	Change Requester

	Activity	Description	Role
3.3.2.3	Peer Review planned change	When the CR is formed and before submitting for formal review (and approval), the details of the change should be peer reviewed. Peer review is a process used for checking the work performed by one's equals (peers) to ensure it meets specific criteria. Peer review is used in working groups for many professional occupations because it is thought that peers can identify each other's errors quickly and easily, speeding up the time that it takes for mistakes to be identified and corrected. In software development teams, the peer review can use a form of code development review, where a team of coders will have a meeting and go through code line by line (even read it aloud possibly) to look for errors. Generally, the goal of all peer review processes is to verify whether the work satisfies the specifications for review, identify any deviations from the standards, and provide suggestions for improvements.	Peer Reviewer

	Activity	Description	Role
3.3.2.4	Submit completed CR for BU review and approval	With corrections made from any areas identified through the peer review and once the CR is ready for submission, the Requester makes the final check for the schedule start date and sets the CR state to Submit. When set to submit, the CR will be auto-routed to the first level of Change Authority review. Depending on if the Requester and Implementer is the same person, there will be a requirement for a peer review of all proposed changes. If the Requester is the one who forms the implementation plan but is not the person who will perform the actual implementation for separation of duties (SoD) or other requirement, the Requester is responsible to have their implementation plan reviewed by a peer. If the Requester is not the one who will develop the implementation plan, the technical peer will need to be performed in a later step.	Change Submitter
3.3.2.5	Review for Accuracy and Approval/Disapproval	All submitted changes must first be fully reviewed for completeness and business purpose for the priority of the change. Only those who are on the approved "Approving Authority" list for their Business Unit (BU) have the rights to approve CRs on behalf of their BU. By approving the CR implies that the Approving Authority is assuming responsibility of the risk and authorization to make the configuration change on behalf of their BU.	BU Level Change Authority

3.3.3. Change Authority (ChM 2.0)

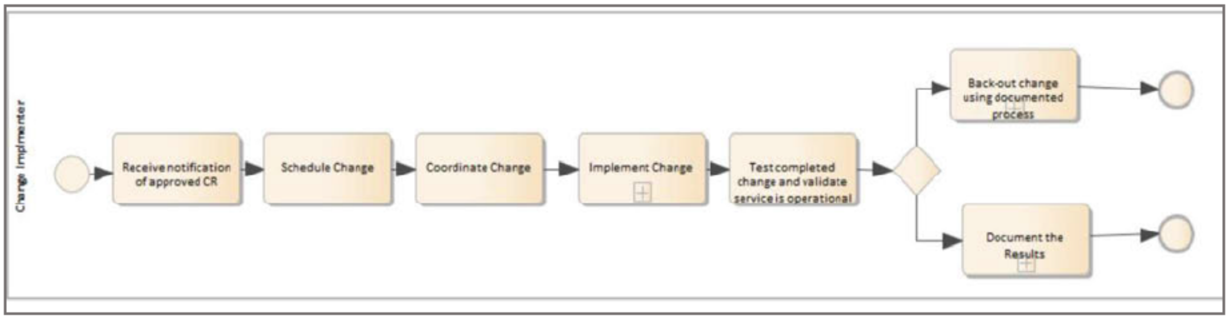

Change Manager
Process Change Request
Determine if higher level Change Authority review is required
Process the approved CR
Assign to Implmenter Ticket Queue
proceed
Change Authority Level-1 to Level-3
Review and make decision
dissaproved

	Activity	Description	Role
3.3.3.1	Process the Change Request (CR) (ChM 2.1)	In this step of a normal change, the CR is routed by the ITSM System[1] to the appropriate change authorities. The routing is based upon the classifications from the CR and on the risk rating related to the change.	Change Management Team
3.3.3.2	Determine if higher level of Change Authority review is required	Follow the established procedure for reviewing the change request in order to determine if the submitted change request contains all requisite information, plans and approvals. Additionally, per the established procedure for evaluating the level of change authority review necessary, make the determination if the submitted change request must be escalated to the next level change authority.	Change Management Team

[1] For purposes of sustainability of this document, the ticketing system used for changes, incidents, service requests, and problems will be referred to as the "ITSM System". As of March 2018, the ITSM System of record will become Changegear.

	Activity	Description	Role
3.3.3.3	Follow escalation procedure for obtaining higher Change Authority approval of a CR	In situations where the next level change authority must evaluate the requested change, the Change Management representative will follow the established procedure for assigning the change request (CR) to the appropriate authority and to communicate that the CR requires further review and evaluation. (Refer to Appendix A of this handbook for more information on change authority levels)	Change Management Team
3.3.3.4	Process the Approved or Disapproved CR	The change management team has established procedures for directing approved changes to the next level of review. In situations where the changes been approved, the change management team will make appropriate notes and move the CR forward. Likewise the change management team has established procedures for handling disapproved changes, which includes making notes inside the CR, notifying the requester that their change has been disapproved, and for setting the correct status of the CR.	Change Management Team
3.3.3.5	Assign to Implementer Ticket queue (ChM 2.5)	This step assumes that the CR has been approved. The change management team will route the CR to the appropriate Implementation Team's CR queue, where is the responsibility of the TR be to review and assigned to the CR if they have approved.	Change Management Team

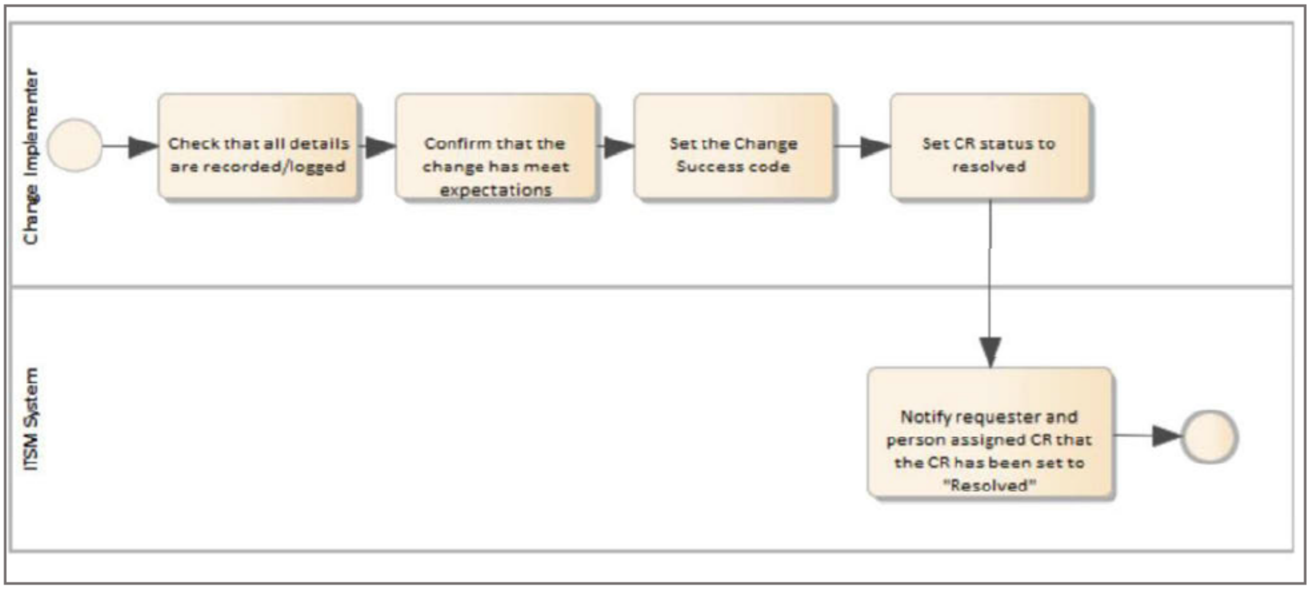
3.3.4. Plan, Schedule and Implement the Change (ChM 3.0)


Change Implmenter
Receive notification of approved CR
Schedule Change
Coordinate Change
Implement Change
Test completed change and validate service is operational
Back-out change using documented process
Document the Results

	Activity	Description	Role
3.3.4.1	Receive notification of approved CR (ChM 3.1)	With the final required approval, the CR is auto-routed to the Implementation Team that is most responsible for implementing the change.	Change Implementer
3.3.4.2	Schedule the change	The Change Implementer reviews the CR and scheduled start date to ensure that they understand the change and the date can be achieved.	Change Implementer
3.3.4.3	Coordinate the Change	If not already assigned, the specific change window (date and time) that the change will be implemented must be confirmed and set.	Change Implementer
3.3.4.4	Implement the change	Follow the implementation plan and related checklist(s), the change is implemented in the assigned change window and per the implementation plan in the approved CR.	Change Implementer
3.3.4.5	Test the completed change and validate the service is operational	In-line with the guidelines established through Software Development Lifecycle (SDLC) and CAB (Change Advisory Board) governance, the appropriate level(s) of testing of the implemented change will be conducted. Process note: As part of testing the completed change, the change implementer or tester will also include steps that validate the service is functioning "normally."	QA or Change Implementer

	Activity	Description	Role
3.3.4.6	Document Results (ChM 3.6)	In situations where the change is implemented successfully, the implementer will follow the activities outlined in their implementation plan and per change management guidelines. Process note: The implementer will notify all stakeholders of the results.	Change Implementer
3.3.4.7	Back-out unsuccessful changes (ChM 3.7)	In rare situations where unacceptable errors or incidents require the change to be reverted, the implementer will follow the activities outlined in their "Back-out" plan (part of the overall implementation plan) and per change management guidelines. Process Note: Any change that is reverted must by definition be considered a "failed change" and this fact must be recorded in the CR. The reason for failure must also be identified and also documented in the CR. Additionally, the implementer will convey the results to stakeholders, to include the summary of why the change had not been successful.	Change Implementer

3.3.5. Document and Communicate the Results (ChM 4.0)


Change Implementer
ITSM System
Check that all details are recorded/logged
Confirm that the change has meet expectations
Set the Change Success code
Set CR status to resolved
Notify requester and person assigned CR that the CR has been set to "Resolved"

No.	Activity	Description	Role
3.3.5.1	Check that all details are recorded and logged (ChM 4.1)	Immediately following any change, the implementer should update the CR with activities performed, the results of the change and all details related to the work that was performed and the results.	Change Implementer

No.	Activity	Description	Role
3.3.5.2	Confirm that the change has met expectations (ChM 4.2)	Gain confirmation from the requester that the change has been successful and meets their expectations. If not already completed, the implementer would also communicate the results of the change to stakeholders as identified in the communications plan for the change. Process note: there will be times when the requester or other stakeholder does not agree with the results from an implemented change, and the arbitration for these situations will be the responsibility of the implementer or their manager. Should need be, the change management team can be engaged to assist with determining the most appropriate course of action.	Change Implementer

No.	Activity	Description	Role
3.3.5.3	Set the change success code (ChM 4.3)	For purposes of collecting metrics and reporting, and in addition to detailed notes added in earlier steps (e.g. 3.3.4.6 and/or 3.3.5.1), the implementer must identify the "success code" for their change. The options available are from the pull-down options to be the one that is most appropriate. The following guidelines apply to the setting of the Change Success: • Successful – No (zero) issues or errors; was not rolled-back; no adjustments had to be made; was completed within the scheduled window for that change request (CR) • Successful with Errors (the change was completed but had issues that required correcting) • Cancelled -- Not performed at all • Unsuccessful – the change failed and needed to be reverted / rolled back to last-known-good-state.	Change Implementer
3.3.5.4	Set CR status to Resolved (ChM 4.4)	As the final step, the CR status will be set to "resolved", and when saved the change and the CR will be considered complete.	Change Implementer

No.	Activity	Description	Role
3.3.5.5	Notification sent to requester (ChM 4.5)	The ITSM System will send an automated notification to the Requester letting them know that the CR was set to resolved. If no issues are identified, the ITSM System will be programed to "close" the CR in 5 days. Process note: As part of a good practice approach to keep accurate historical records, once closed, no ticket (CR, Incident, Request, etc.) is "reopened". Should further work or rework be required after the ticket is closed, a new ticket (CR, Incident, request, etc.) will be required with updated information and as necessary, new approvals.	ITSM System

4. Roles and Responsibilities

A **role** refers to a set of connected behaviors or actions that are performed by a person, team or group in a specific context. Process roles are defined by the set of responsibilities, activities and authorities granted to the designated person, team or group. Roles associated with the Requirements Management process are defined in the context of the management function and are not intended to correspond with organizational job titles.

All roles and designated person(s), team(s), or group(s) should be clearly communicated across the organization. This should encourage or improve collaboration and cooperation for cross-functional process activities

Role	Definition
Process Owner	The change management process owner is the person who is most accountable for the management and continual improvements of the change management process.
Responsibilities	
▪ Sponsoring, designing and change managing the process and its metrics ▪ Defining the process strategy ▪ Assisting with process design ▪ Ensuring that appropriate process documentation is available and current ▪ Defining appropriate policies and standards to be employed throughout the process ▪ Periodically auditing the process to ensure compliance to policy and standards	

Role	Definition
▪ Periodically reviewing the process strategy to ensure that it is still appropriate and change as required ▪ Communicating process information or changes as appropriate to ensure awareness ▪ Providing process resources to support activities required throughout the service lifecycle ▪ Ensuring process technicians have the required knowledge and the required technical and business understanding to deliver the process, and understand their role in the process ▪ Reviewing opportunities for process enhancements and for improving the efficiency and effectiveness of the process ▪ Addressing issues with the running of the process ▪ Identifying improvement opportunities for inclusion in the **continual service improvement** (CSI) register ▪ Working with the CSI manager and process manager to review and prioritize improvements in the CSI register ▪ Making improvements to the process. ▪ Designing change authority hierarchy and criteria for allocating CRs to change authorities ▪ Designing change models and workflows ▪ Working with other process owners to ensure that there is an integrated approach to the design and implementation of change management, service asset and configuration management, release and deployment management, and service validation and testing.	
Process Manager	The change process manager is the person who is most responsible for the management and continual improvements of the change management process.
Responsibilities	
• Work with the process owner to plan and coordinate all process activities • Ensuring all activities are carried out as required throughout the service lifecycle • Appointing people to the required roles • Managing resources assigned to the process • Working with service owners and other process managers to ensure the smooth running of services • Monitoring and reporting on process performance • Identifying improvement opportunities for inclusion in the CSI register • Working with the CSI manager and process owner to review and prioritize improvements in the CSI register • Making improvements to the process implementation. • Carrying out the generic process manager role for the incident management process • Planning and managing support for change management tools and processes • Maintaining the change schedule and projected service outage • Coordinating interfaces between change management and other processes – especially service asset and configuration management and release and deployment management.	
Change Manager	This is a role for a person who is responsible for the over sight and management of change requests (CRs) as they progress through the change lifecycle. This role is generally performed by the Change Management process manager but in

Role	Definition
	organizations where someone other than the Process Manager is responsible for the change requests, this role can be assigned to someone other than the process manager. This role is part of the Change Management Team
Responsibilities	
• Review specific categories of CR • Notifying Change Requesters, Change Implementers, Change Practitioners when their CR requires additional information. • Reviewing and authorizing changes at agreed points in the change lifecycle • Participate in change and release planning • Participate in the change review before changes are closed • Attend CAB meetings to discuss and review changes when required.	
Change Coordinator	This is a role for the person who is responsible for the day-to-day support and processing of change requests (CRs) as they progress through the change lifecycle. This role is a backup for the Change Manager and is formally part of the Change Management Team.
Responsibilities	
• Review specific categories of CR • Notifying Change Requesters, Change Implementers, Change Practitioners when their CR requires additional information. • Reviewing and authorizing changes at agreed points in the change lifecycle • Participate in change and release planning • Participate in the change review before changes are closed	
Change Requester	Many different people in the organization may carry out this role; it is not usually carried out by people who work in change management. Each change will only have a single change requester. This person initiates a CR, and may reside within the business unit or the IT organization. Often, but not always, the requester and the implementer of a change are the same person. In larger organizations and/or in certain situations (e.g. big releases, infrastructure projects, etc.) someone else may create the CR to make the proposed change visible on the change schedule while a different person or team will implement the change.
Responsibilities	
• Identifying the requirement for a change • Completing and submitting a change proposal if appropriate • Developing and providing an implementation plan if necessary • Completing and submitting an CR • Attending CAB meetings to provide further information about the CR or change proposal if invited	

Role	Definition
• Reviewing change when requested by change management, and specifically before closure.	
Change Practitioner	A role held by a member of the change management team
Responsibilities	
• Verifying that RFCs (requests for change) are correctly completed • Allocating RFCs to appropriate change authorities based on defined criteria • Submitting requests for evaluation to trigger the change evaluation process • Formally communicating decisions of change authorities to affected parties • Monitoring and reviewing activities of teams and functions that build and test changes to ensure that the work is carried out correctly. (This will be carried out as part of the release and deployment management process for a change that is part of a release.) • Publishing the change schedule and projected service outage and ensuring that they are available when and where needed.	
Change Advisory Board (CAB) Chair	DMDC will utilize multiple levels of change authority and at the Divisional level, the change authority is represented by a formal Change Advisory Board (CAB). The CAB Chairperson will be an assigned role. As there will be multiple change authorities, there will be a chairperson for each board or committee form to perform change authority responsibilities. (See Appendix A, for more information on the plan for the change advisory board.)
Responsibilities	
• Deciding who should attend CAB meetings • Planning, scheduling, managing and chairing CAB meetings • Selecting CRs for review at CAB meetings, based on the change policy • Circulating CRs in advance of CAB meetings to allow prior consideration • Convening emergency change advisory board (ECAB) meetings for consideration of emergency changes • Selecting successful and failed changes for review at CAB meetings.	
CAB Member	This person attends scheduled meetings or sends a representative, and is empowered to make decisions on behalf of the business unit, group or organization that he or she represents. The CAB may ask participants to take on responsibilities such as a change technical reviewer — a CAB member who provides technical guidance during CAB assessment and authorization stages of one or more CRs. This role usually requires broad business and technical knowledge from the overall IT service to the CI level.
Responsibilities	
• Participating in CAB meetings • Authority to represent a particular group or function • Preparing for CAB meetings by circulating CRs within their own group and coordinating feedback • Reviewing CRs and recommending whether they should be authorized	

Role	Definition
• Reviewing successful and failed changes • Reviewing unauthorized changes • Reviewing the change schedule and providing information to help identify conflicts or resource issues • Reviewing the projected service outage and providing feedback on the impact of planned outages.	
Change Authority	There will normally be different change authorities for each category of change. See the section on Change Authorities for more information about change authorities. For DMDC, Change Authorities will include CAB Chairs, the IT Operations Director, Information Assurance (aka: Cyber Security Division) and approvers at the business unit level (aka: Business Unit Approvers) would be considered a change authorities.
Responsibilities	
The change authority's responsibilities typically include: • Reviewing specific categories of RFCs • Reviewing CRs where appropriate • Formally authorizing changes at agreed points in the lifecycle of a change • Participating in the evaluation and review of changes before the CR is closed • Attending CAB meetings to discuss and review changes when required.	
Service Owner	The service owner is accountable for the delivery of a specific IT service. The service owner is responsible to the customer for the initiation, transition and ongoing maintenance and support of a particular service and accountable to the IT director or service management director for the delivery of the service. The service owner's accountability for a specific service within an organization is independent of where the underpinning technology components, processes or professional capabilities reside. The service owner is responsible for continual improvement and the management of change affecting the service under their care. The service owner is a primary stakeholder in all of the underlying IT processes which enable or support the service they own.
Responsibilities	
• Ensuring that the ongoing service delivery and support meet agreed customer requirements • Working with business relationship management to understand and translate customer requirements into activities, measures or service components that will ensure that the service provider can meet those requirements • Ensuring consistent and appropriate communication with customer(s) for service related inquiries and issues • Assisting in defining service models and in assessing the impact of new services or changes to existing services through the service portfolio management process • Identifying opportunities for service improvements, discussing these with the customer and raising RFCs as appropriate • Liaising with the appropriate process owners throughout the service lifecycle • Soliciting required data, statistics and reports for analysis and to facilitate effective service monitoring and performance	

Role	Definition
	• Providing input in service attributes such as performance, availability etc. • Representing the service across the organization • Understanding the service (components etc.) • Serving as the point of escalation (notification) for major incidents relating to the service • Representing the service in change advisory board (CAB) meetings • Participating in internal service review meetings (within IT) • Participating in external service review meetings (with the business) • Ensuring that the service entry in the service catalog is accurate and is maintained • Participating in negotiating SLAs and operational level agreements (OLAs) relating to the service • Identifying improvement opportunities for inclusion in the continual service improvement (CSI) register • Working with the CSI manager to review and prioritize improvements in the CSI register • Making improvements to the service.

5. RACI Authority Matrix

The purpose of the Responsible, Accountable, Consulted, and Informed (RACI) matrix is to document the activities and roles and sufficiently define the Responsible, Accountable, Consulted, Informed participation level. This authority matrix identifies high-level process activities that can be associated with key roles. This table is to be leveraged to create and map specific activities to specific DMDC ITSM organizational roles.

Process Activities	Process Owner	Process Manager	Change Advisory Board
Ensures detailed processes are developed, implemented and improved for DMDC based on this guidance	R	C	C
Ensure that culture change is managed so that the organization is prepared to accept the new ChM process.	R	C	I
Ensures that processes and procedures are standardized and aligned with other ITSM service provider processes and clear process inputs/outputs are recognized and defined	R	C	C
Ensures that the ChM process is developed, optimized and aligns with ITSM service provider policies and procedures	A	R	C
Ensures that process is developed and implemented to consistently record, assess and prioritize change requests	A	R	R

Process Activities	Process Owner	Process Manager	Change Advisory Board
Assess impact and prioritize changes based on business and mission needs	C, I	A, R	R
Assure that any emergency and critical change follows the approved process	C, I	A, R	R
Authorize changes	I	A, R	C
Manage and disseminate relevant information regarding changes	I	A, R	C
Produce management reporting	A	R	C
Produce process implementation progress/KPI reports	R	R	C

6. Meetings

For the change management process and related communications to be effective, specific meetings that follow a defined agenda must occur on a regular basis. All attendees of each meeting should be aware of the meeting's goals; objectives, expected outcomes and the change manager should track and publish meeting minutes. Attendees should be clear on their roles, to include being able to clearly speak to the impact of any CR they represent, as well as being able to answer questions around the execution of the change including, but not limited to personnel logistics, inter-CR dependencies, and testing and rollbacks of more complex changes.

Meetings that will be scheduled by the Change Management Team include:

- **Short Term Planning Meeting:** This is a planning session occurring every Tuesday at 10:10 AM Pacific time. These planning sessions are used to review and answer questions about the execution of all planned patching changes scheduled for the next maintenance window.
- **Pre-Weekend Maintenance (aka: Pre-Flight) Meeting:** This is a planning session occurring every Thursday where a maintenance will be held. These pre-implementation sessions are used to review and answer questions about the execution of all planned changes and releases scheduled for the upcoming weekend's maintenance window.

7. Performance Metrics

Important to ensuring service quality and to enable continual process improvement, the organization must be able to measure the impact that changes have on service delivery. If the

ChM process is efficient and effective, measurements of the ChM process should demonstrate reduced disruption over time and identify the speed and effectiveness with which the service delivery groups are able to respond to identified business needs.

Based upon best practices and an assumed maturity level of one[2], the Change Management (ChM) process will initially be measured by the Critical Success Factors and Key Performance Indicators identified in this document. As the process matures reducing the need to track these KPI as performance measures and/or the need to track others increases, the CSF/KPI tracked for purposes of measuring the ChM process might be different.

Assumptions:

- The process is defined, documented and executive support for the process is consistently strong
- Training has been provided for all implementers and requesters
- The ITSM System (aka: tool) used for recording and managing changes is appropriate for ITSM Change Management, it is aligned with the process, is integrated with the other ITSM processes and that the tool is supported.
- All changes must be recorded in the ITSM System
- Data can be readily exported from the ITSM System
- Reports will be provided on a monthly basis, with month-on-month trending tracked and also reported
- Analysis will be provided based upon data

No	CSF	KPI	Description	Use
1	Controlling Changes	Total number of changes implemented	Total count of authorized changes implemented	Used as part of performance reporting of volume and also for comparison with other KPI
2	Processing Change Requests	Total number of Change Requests (CR) processed	Total count of CRs processed	Identify the number of changes proposed as a measure of support required from ChM and

[2] Maturity based upon the ITIL Maturity model. More information can be found on the Axelos site: https://www.axelos.com/best-practice-solutions/itil/itil-maturity-model

No	CSF	KPI	Description	Use
				other change reviewers, etc.
3	Making Quick and Accurate Changes Based on Business Priorities	Percentage of successful changes	Following implementation of any change, the implementer must update the "change success" field in the CR with the results of the change	This is a measurement of how effective planning and preparation is of changes implemented.
4	Making Quick and Accurate Changes Based on Business Priorities	Number of changes determined to not having been successful than successful	Following implementation of any change, the implementer must identify if their change was less than successful as defined within the ChM documentation.	This is a measurement of how effective planning and preparation is of changes implemented.
5	Making Quick and Accurate Changes Based on Business Priorities	Number of changes that are classified as "Emergency" (Compared against the total number of implemented changes in the same time period being measured (week, month, year))	Only changes that are required to restore a failed service or adversely impacted service will be classified as "emergency". There must be an active incident and need to immediately repair the impacted service for the change to be considered an "emergency". This type of change is most often used during a high severity major incident (aka: SRT)	The number of emergency changes should be relatively low as this reflects the number of changes that must be applied to 'fix' an adversely impacted service. The higher the percentage, the greater the concern should be with why there is a high volume and need for emergency changes.

No	CSF	KPI	Description	Use
6	Making Quick and Accurate Changes Based on Business Priorities	Number of changes that are classified as "Critical" and/or "Urgent" (aka: elevated priority) (Compared against the total number of implemented changes in the same time period being measured (week, month, year))	This measurement provides visibility to the percentage of changes requested with elevated priority as compared to "routine" (aka: "normal" within ITSM) priority changes	The number of elevated priority changes should be relatively low as this reflects the number of changes that must be applied quickly into DMDC controlled environments. With "speed" comes greater risk and likely far less quality assurance support for a change, and therefore this number should always be low. The higher the percentage, the greater the concern should be with if there is a planning and/or performance issue that is causing the organization(s) to speed changes into environments (aka: regions)
7	Protecting Services When making Changes	Percent and number of changes that result in an incident	Any service outage or disruption identified to be as a result from a change will be measured by incidents.	Provides visibility of changes that are made and result in incidents to DMDC environments (aka: regions).

No	CSF	KPI	Description	Use
8	Protecting Services When making Changes	Percent and number of changes that are backed out	This is to track any change that must be "backed out" (aka: rolled back)	Provides visibility to the Changes that don't produce the results planned in the RFC.

Achievement against KPIs will be monitored and used to identify opportunities for improvement, which will be logged in the CSI register for evaluation and possible implementation.

8. ChM Interfaces with Other Processes

All service management processes may require change management, for example to implement process improvements. Many service management processes will also be involved in the impact assessment and implementation of service changes, as discussed below.

Process	Details
IT Service Continuity Management	IT service continuity management has many procedures and plans, which should be updated via change management to ensure that they are accurate and up to date, and that stakeholders are aware of changes. Every change should be assessed for its impact on IT service continuity arrangements. For a standard change this will be done at the time the change model is authorized; for normal and emergency changes the assessment will be done as part of change assessment.
Release and Deployment Management	Release and deployment management must be tightly integrated with change management. Change management provides the authorization for the work that is carried out by release and deployment management, and release and deployment management provides the actual execution of many changes. Release and deployment plans are a significant part of the change schedule, and these must be managed together. Every deployment must be reviewed and closed
Service Asset and Configuration Management	The configuration management system provides reliable, quick and easy access to accurate configuration information to enable stakeholders and staff to assess the impact of proposed changes and to track change work flow. This information enables the correct CI versions to be released to the appropriate party or into the correct environment. As changes are implemented, the configuration management information is updated. The CMS may also identify related CIs that will be affected by the change, but not included in the original request, or similar CIs that would benefit from similar changes.

Problem Management	Problem management is another key process, as changes are often required to implement workarounds and to fix known errors. Problem management is one of the major sources of RFCs and is also often a major contributor to CAB discussion.
Information Security Management	Information Security Management[3] interfaces with change management, since changes required by security will be implemented through the change management process and security will be a key contributor to CAB discussion on many services. Every significant change will be assessed for its potential impact on information security management.
Capacity Management	Capacity management and demand management are critical aspects of change management. Poorly managed demand is a source of cost and risk for service providers because there is always a level of uncertainty associated with the demand for services. Capacity management has an important role in assessing proposed changes – not only the individual changes but the total impact of changes on service capacity. Changes arising from capacity management, including those set out in the capacity plan, will be initiated as RFCs through the change process.
Service Portfolio Management	The service portfolio management process prioritizes and charters strategic changes, and submits change proposals for these. Change proposals will be a significant input to long-term planning for the change schedule, and will also be a key input to help change management review and authorize related RFCs. Some change requests will require analysis by the service portfolio management process, potentially adding to the service pipeline. Each organization should define criteria for deciding whether these requests are managed as part of the change management process or are passed to service portfolio management.

9. Information Management

All CRs must be associated with services and other CIs. This means that either they must be included within the ITSM System or a mechanism must be provided to enable cross referencing and searching changes related to CIs. It is essential for a single tool (ITSM System) to be used for managing incidents, problems and changes, as well as the CMS (configuration management

[3] ITSM best practices and in particular ITIL, includes the Information Security Management (ISM) process, which for DMDC is handled by the Cyber Security Division (CSD). For purposes of this Handbook, the reference to ISM is included in this section but it is important to note and acknowledge that the ISM function within the ChM process and the CAB will be represented by CSD personnel.

information), and a highly integrated ITSM System can help to improve the efficiency of the ITSM processes.

It is very important to be able to correlate changes with incidents and to review the history of changes to any CI as part of incident or problem management. This requires access to historical change information, which should be made available for searches.

Change management must have access to dependency and relationship information found within the CMDB and to information and documents within the SKMS in order to plan and manage changes, to identify stakeholders in any change, and to predict the potential impact of changes.

10. Appendices

Appendix A: Change Authority

Formal authorization is obtained for each change from a change authority that may be a role, person or a group of people that are formed into a "change advisory board", or CAB.

As an additional and critical factor of the ChM process, the EGC (DMDC's Executive Governance Committee) directed that levels of change authority be developed and implemented along with the improved ChM process. To fulfill this requirement, and to ensure that decision-making is delegated to the lowest possible level, the change authority model to be implemented provides for at least 4 levels of decision making.

The authorization for a particular type of change will be judged based on the type, cost, risk and potential business impact of the change, for example: major changes that will affect several DMDC external customers, may need to be authorized by a higher-level change authority such as an Enterprise (level-2) CAB. Another example might be a fundamental change to the DMDC service architecture, which by best practice would require "Executive CAB" approval. (Where the Executive (level-1) CAB is formed at the DMDC Directors level, and only the Executive CAB can make that type of decision.)

DMDC CAB Scope and Change Authority Levels

[4]The scope of DMDC change authority is a multi-level review and approving authority for changes to DMDC infrastructure and configurations. The Change Authority responsibilities include all DMDC configurations, assets, environments and regions that are established in the approved charters for the Change Management (ChM) and

[4] As of January 2018, the CAB charters have not yet been approved and published. This section has been added to this change management process handbook for purposes of informing the reader of the intent of the change advisory board (CAB). At the time the CAB charter is fully reviewed and approved, this section of the change management process handbook will be updated to align with the approved charter. For more information on the proposed CAB charter, contact the change management process owner.

Configuration Management (CfM) processes. Based upon criteria included in this document and with increasing levels of responsibilities that include:

- Review and approval of requests for new services
- Review and approval for requests to change approved architectures and standards
- As necessary, review and approval of changes to configurations based upon cost, risk and potential for service interruptions
- Review and inputs to Continual Service Improvement (CSI) on the performance of DMDC change, release and configuration management processes

Levels of Change Authority

Formal authorization must be obtained for each change from a change authority that has been established as part of the enterprise ChM program. The level of authorization required for each change is determined by the type, size, risk and potential business impact of the change, e.g. changes to DMDC infrastructure or software standards need to be authorized by the top-level change authority for DMDC (aka: Change Authority Level-1)

To provide for decision making at the lowest possible level within the organization, while also providing the essential structure for escalating conflicts or risk acceptance, DMDC leadership provides three official Change Authority levels of governance, one Directorate level authority and one local level of authority for configuration changes. A fundamental tenant of multi-level change authority is to facilitate the necessary review of change at the lowest possible level in the organization, while still providing for escalation of decisions through increasing levels of authority. For example, if change assessment at level 2 or 3 detects higher levels of risk, the authorization request is escalated to the appropriate higher level for the assessed level of risk. The level at which change is authorized should rest where accountability for accepting risk and remediation exist.

Change Authority Level-1

Level-1 is the Enterprise CAB and is comprised of senior DMDC decision makers.[5]

Change Authority Level-2

Level-2 is represented by Technical Services and other directorate representatives

[5] As of January 2018 the composition of the Level I cab has not yet been determined. It is conceivable that the level I cab would be the same decision-making body for new services or architectural changes or could be represented by existing DMDC's existing decision-making groups like the Enterprise Governance Committee (EGC).

Change Authority Level-3

Level-3 is represented by the Change Management Process Manager.[6]

Change Authority Level-4

The Level-4 Change Authority represents the approving authority held by Directorate leaders over changes to services and applications they are responsible for.

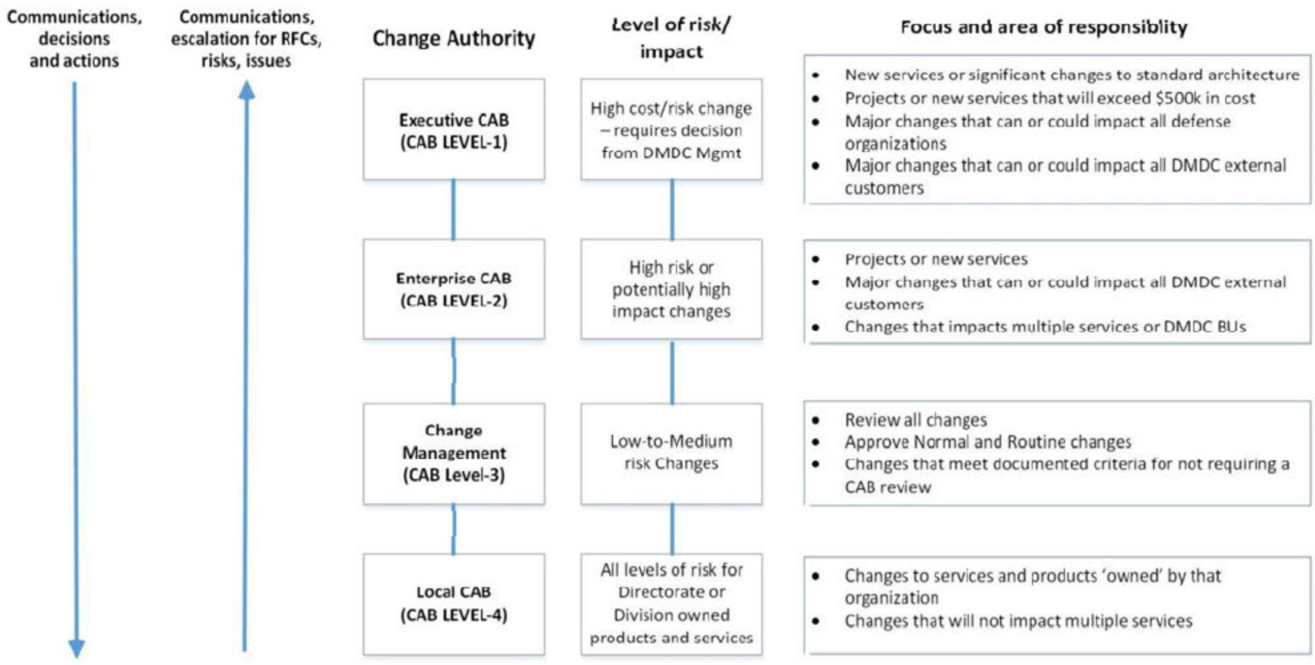
Also known as "Approving Authority", the Level-4 approvers are formed from leaders from Division or Directorate groups and they are responsible for reviewing those change requests (CR) that have the potential to affect their immediate areas of support or responsibility. It is important to note that this level of Change Authority do not provide final approval, however they by approving a CR confirms their Directorate agrees with and they accept the risk associated with the deployment or change to be implemented.

The final approval for all changes rests with one of the three higher level change authority groups

For DMDC, the following figure represents the levels of Change Authority. [7]

[6] The CAB delegates a degreed of authority to the change manager which effectively make the Change Manager the Level-3 Change Authority. The use of delegated authority from higher levels to process teams must be accompanied by trust in the judgement, access to the appropriate information and supported by DMDC Governance leadership.

[7]


Communications, decisions and actions
Communications, escalation for RFCs, risks, issues

Change Authority	Level of risk/ impact	Focus and area of responsiblity
Executive CAB (CAB LEVEL-1)	High cost/risk change – requires decision from DMDC Mgmt	• New services or significant changes to standard architecture • Projects or new services that will exceed $500k in cost • Major changes that can or could impact all defense organizations • Major changes that can or could impact all DMDC external customers
Enterprise CAB (CAB LEVEL-2)	High risk or potentially high impact changes	• Projects or new services • Major changes that can or could impact all DMDC external customers • Changes that impacts multiple services or DMDC BUs
Change Management (CAB Level-3)	Low-to-Medium risk Changes	• Review all changes • Approve Normal and Routine changes • Changes that meet documented criteria for not requiring a CAB review
Local CAB (CAB LEVEL-4)	All levels of risk for Directorate or Division owned products and services	• Changes to services and products 'owned' by that organization • Changes that will not impact multiple services

11. References

- DoDI 8500.01, Cyber Security Policy, dated March 14, 2014
- DoD Information Technology (IT) Service Management (ITSM) DoD-I, 8440.01 December 24, 2015
- DoD Enterprise Service Management Framework, Edition III, signed June 16 2016
- DMDC Change Advisory Board Charter, November 2017
- DMDC Change Advisory Board Guidebook, November 2017
- DMDC Technical Review Board (TRB) Charter, June 2017
- DMDC ITSM Technical Review Board (TRB) and Change Control Board (CCB) Process document, June 2017
- DMDC Change Request Users Guide, v2.9, dated: 10 November 2017
- ITIL Service Design, TSO, v2011
- ITIL Service Transition, TSO, v2011
- ISO/IEC 20000-1:2011, Clause 5
- Control Objects for Information and Related Technology (COBIT) v5, BAI06

12. Glossary

The terminology and definitions specific to this process document can be found on the BPR SharePoint:

http://mydmdc/restructure-2017/Business%20Process%20Review/Lists/DMDC%20BPR%20Glossary/Display%20View.aspx